Fact Sheet: Suspicious Activity Reporting (SAR) Functional Standard for the Information Sharing Environment

"The attacks of September 11 illustrated that foreign terrorists wanting to commit acts of terrorism might live in our local communities and be engaged in criminal or other suspicious activity as they plan attacks on targets within the United States or its territories. . . . Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by State, local, and tribal government personnel in the course of routine law enforcement and other activities."

– National Strategy for Information Sharing, October 2007

First Version of ISE-SAR Functional Standard Released

➢ On January 25, 2008, Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment (ISE), issued the first version of the ISE – Suspicious Activity Reporting (SAR) Functional Standard (ISE-FS-200).

➢ The ISE-SAR Functional Standard will support the sharing between Federal, State, local and tribal partners, of suspicious activity or incident information with a potential terrorism nexus, in a manner that protects the privacy and legal rights of Americans.

➢ The effective sharing of ISE-SAR will enable the discovery and analysis of potential terrorism-related patterns or trends on a regional and national basis beyond what would be recognized within a single organization, jurisdiction, State, or territory.

➢ This functional standard supports implementation of the President's *National Strategy for Information Sharing* which identifies Suspicious Activity Reporting as one of the key information exchanges between the Federal Government and our State and local partners.

State and Major Urban Area Fusion Centers Key Partners in ISE-SAR Process

➢ Standardized and consistent sharing of suspicious activity information with State and major urban area fusion centers is integral to assessing, deterring, preventing, or prosecuting those planning terrorist activities.

➢ The ISE-SAR Functional Standard can be used by non-Federal ISE participants, such as State and major urban area fusion centers, and State, local, and tribal law enforcement and homeland security organizations.

➢ Consistent with Guideline 1 of the President's Memorandum of December 2005, *Guidelines and Requirements in Support of the Information Sharing Environment*, and the *Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act),* the Department of Homeland Security and the Department of Justice are responsible for making this and other Common Terrorism Information

Sharing Standards (CTISS) available for use by State, local, and tribal governments and the private sector, and requiring its use through grant guidance and other mechanisms, as appropriate.

ISE-SAR Functional Standard

➢ Suspicious Activity Reporting (SAR) is the process of documenting the observation of behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intentions.

➢ Any suspicious activity report that is determined to have a potential nexus to terrorism should be designated an ISE suspicious activity report.

➢ The ISE-SAR Functional Standard documents information sharing exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SAR by ISE participants.

  ▪ This initial version of the functional standard will continue to be tested and evaluated by the user community. Any resulting refinements to the ISE-SAR business processes and data elements will be incorporated in future versions.

  ▪ Privacy assessments will also be performed, as appropriate, to identify privacy issues that may arise in implementing the proposed functional standard and information flow.

➢ The functional standard is not intended to address all implementation issues associated with the reporting, tracking, processing, access, storage, and retrieval of SAR information within the ISE. This ISE-SAR Functional Standard is one component of the overall ISE-SAR initiative.

➢ The ISE-SAR Functional Standard was developed through a collaborative process involving the Information Sharing Council as well as State and local law enforcement and homeland security representatives.

➢ The ISE-SAR Functional Standard contains the following major elements:

  ▪ List of Information Exchange Artifacts – The information exchange provides details of implementation processes, and tangible information sharing technical products such as standards compliant data models and system interface schemas.

  ▪ SAR Exchanges – A high level, top down description of the ISE-SAR exchanges with Purpose, Scope, and Top-level Business Process and Activities.

  ▪ ISE-SAR Exchange Data Model – A comprehensive inventory of all ISE-SAR information exchange data classes, elements, and definitions. A privacy field allows for information to be excluded from summary ISE-SAR.

  ▪ ISE-SAR Selection Criteria Guidance – There are 18 initial categories identified as part of the ISE-SAR selection criteria guidance. Each category is given a definition.

- Activities in Suspicious Activity Reporting Information Flow – Nine steps are depicted in the ISE-SAR Information Flow. A diagram connecting these activities is also included.

The Common Terrorism Information Sharing Standards Program

➢ On October 31, 2007, Ambassador McNamara established the CTISS program (ISE-AM-300) consistent with the direction provided by the President in Guideline 1 of his December 2005 Memorandum, and section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

➢ CTISS are business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS:

- Functional Standards – Functional standards describe the rules, conditions, guidelines and characteristics of focused mission areas that use ISE business processes and information exchanges to share information.

- Technical Standards – Technical standards document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.

➢ The issuance of the ISE-SAR Functional Standard constitutes the first of the CTISS issued by the PM-ISE. Its official designation is ISE-FS-200 and can be retrieved, in its entirety through the CTISS Page of the ISE website: www.ise.gov.

Information Sharing Environment Background

➢ The *Intelligence Reform and Terrorism Prevention Act* of 2004, as amended by the *9/11 Commission Act,* calls for the development of an ISE to facilitate the sharing of terrorism and homeland security information among Federal, State, local, and tribal governments and, as appropriate, foreign partners and the private sector.

➢ The Information Sharing Council was directed by the *Intelligence Reform and Terrorism Prevention Act of 2004* and established by Executive Order 13388 to advise the President and the Program Manager, Information Sharing Environment, and to provide for coordination among the federal agencies participating in the ISE.